Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

June 2016

Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the State Office of Cyber Security, Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington State's security posture.

The goal of the tabletop exercise is to increase security situational awareness and to facilitate discussion of incident response in as simple a manner possible; targeting a time range of 15 minutes. The exercises provide an opportunity for management to present realistic scenarios to a workgroup for development of response processes.

How to best use the tabletop exercise:

1. Modify the tabletop scenario as needed to conform to your environment.

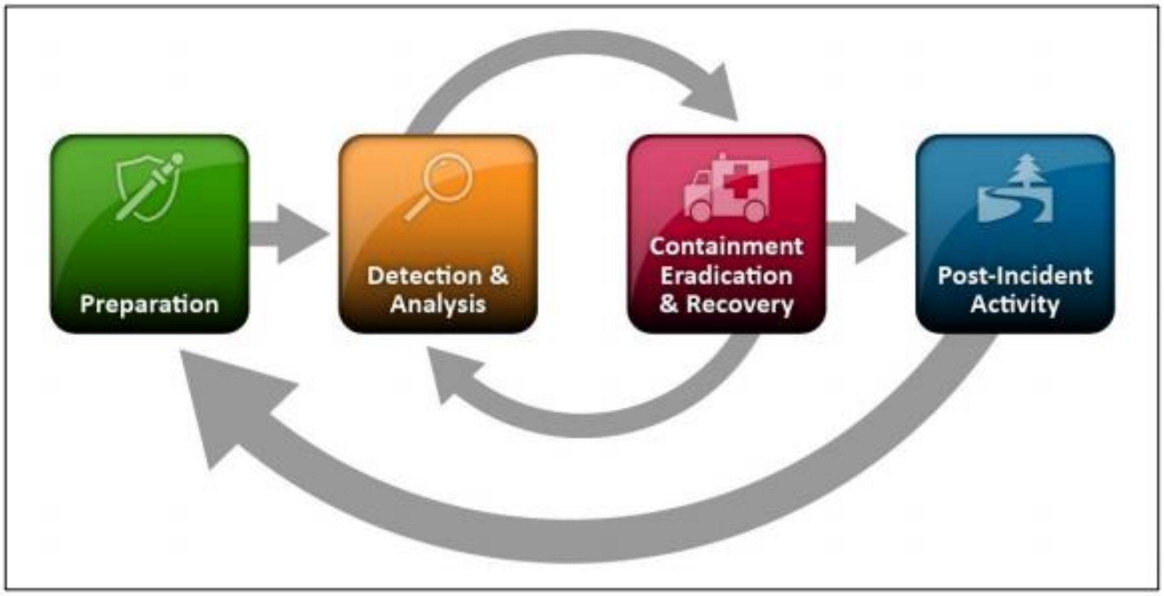
2. Engage management.

3. Present scenario to the workgroup.

4. Discuss the process to address the scenario.

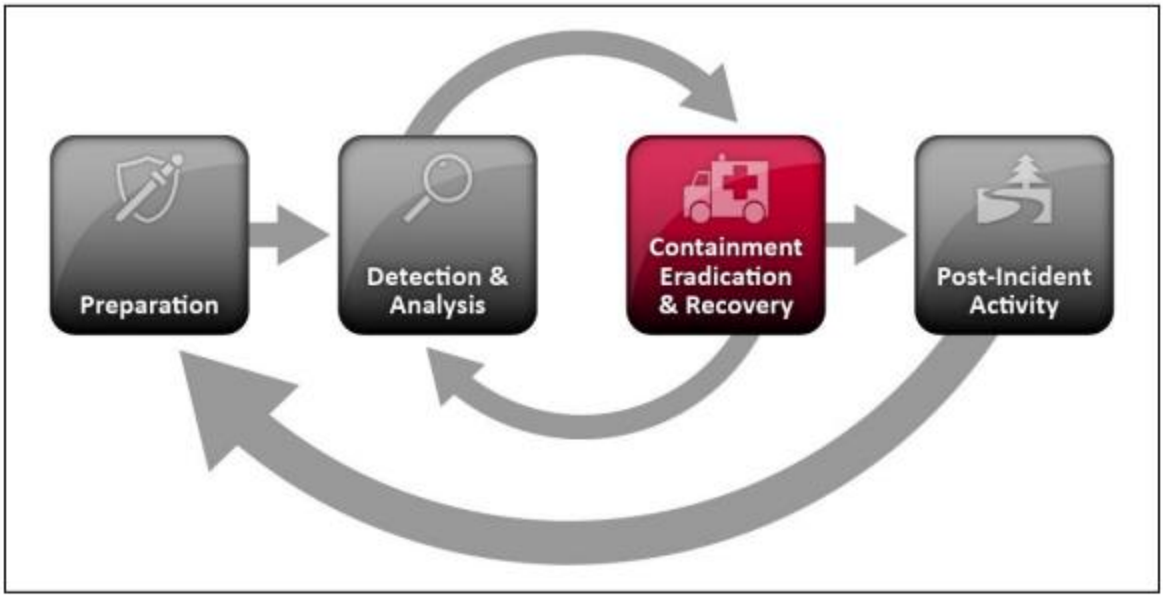
5. Document the response and findings for future reference

Note: A member of the State Office of Cyber Security, Security Operations Center will be happy to facilitate this exercise with a workgroup from your agency upon request to the WaTech Service Desk at 360-753-2454.



EXERCISE SCENARIO

On a Saturday afternoon, external users start having problems accessing the organization's public websites. Over the next hour, the problem worsens to the point where nearly every access attempt fails. Meanwhile, a member of the organization's networking staff responds to alerts from an Internet border router and determines that the organization's Internet bandwidth is being consumed by an unusually large volume of User Datagram Protocol (UDP) packets to and from both the organization's public DNS servers. Analysis of the traffic shows that the DNS servers are receiving high volumes of requests from a single external IP address. Also, all the DNS requests from that address come from the same source port.

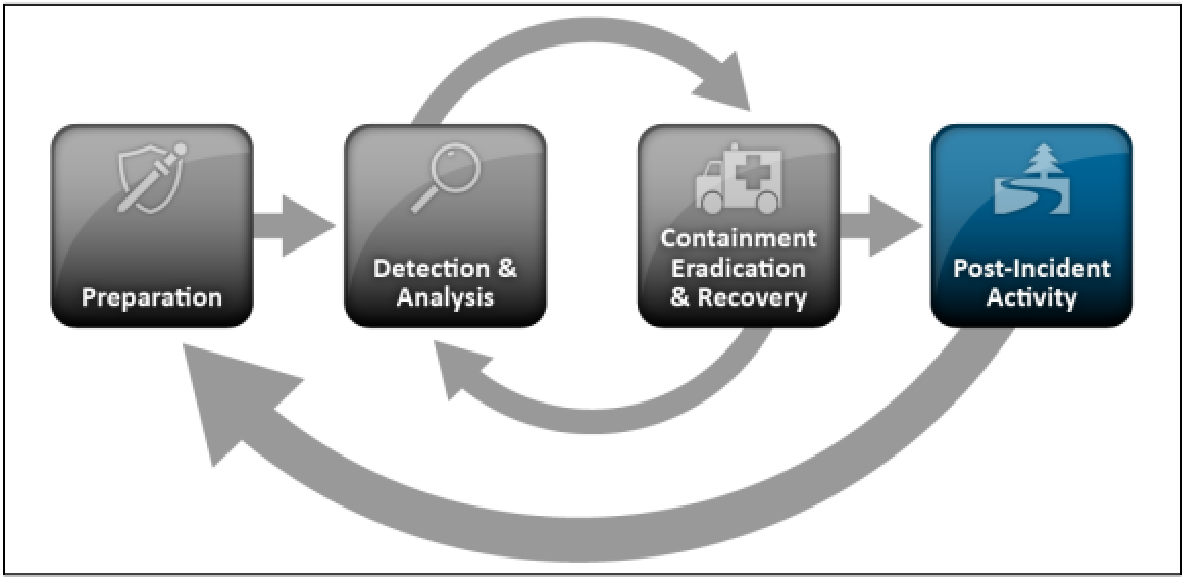


ITEMS TO DISCUSS

- Whom should the organization contact regarding the external IP address in question?
- Suppose that after the initial containment measures were put in place, the network administrators detected that nine internal hosts were also attempting the same unusual requests to the DNS server. How would that affect the handling of this incident?
- Suppose that two of the nine internal hosts disconnected from the network before their system owners were identified. How would the system owners be identified?

ITEMS TO REPORT

- Did communications flow as expected? If not, why?
- Were processes and procedures followed?
- Were there any surprises?
- How well did the exercise work for your organization?



CONTACT US

The State Office of Cyber Security SOC forms a focal point for the efficient reporting, containment, and recovery of security incidents.

To report a cyber-incident, contact the WaTech Service Desk at (360) 753-2454 / 1-888-241-7597.

For general questions, send us an email at soc@watech.wa.gov.

For more information, visit our site at: http://www.soc.wa.gov.

The State Office of Cyber Security, Security Operations Center (SOC) is an active member with the Multi-State Information Sharing and Analysis Center (MS-ISAC) which has been designated by the US Department of Homeland Security (DHS) as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. Through this relationship, the State Office of Cyber Security SOC is able to leverage resources available from MS-ISAC of malware analysis, reverse engineering, log analysis, and forensics analysis in a cyber incident.

The mission of the State Office of Cyber Security SOC is to provide centralized information sharing, monitoring, and analysis of Washington State's security posture. The promotion of cyber security education and awareness to end users is critical to maintenance of a strong security posture of the Washington State network.

Security Operations